REMARKS

These remarks follow the order of the paragraphs of the office action. Relevant portions of the office action are shown indented and italicized.

Claims 1-15 remain in the application. New claims 16-20 are added to better protect thye invention for the applicants.

DETAILED ACTION

Claim Rejections 35 US §102

> *The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:*
> *A person shall be entitled to a patent unless —*
> *(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than, one year prior to the date of application for patent in the United States.*
>
> *Claims 1-15 are rejected under 35 U.S.C. 102(h) as being anticipated by S. Ma, et al., "EventMiner" : An integrated mining tool for Scalable Analysis of Event Data", May 21. 2001, www.research.ibm.com.*

In response, applicants respectfully state that the present invention is not anticipated by S. Ma, et al. The present invention provides methods for monitoring events in a computer network, said computer network triggering said events, wherein each event is provided with attribute values allocated to a given set of attributes. It provides methods, apparatus and systems for monitoring events in a computer network **enabling an operator of an intrusion-detection system to simultaneously monitor various event attributes versus the arrival time of the events**.

The cited reference, S. Ma, et al., indeed presents other event mining methods. That visualization method using a two-dimensional mapping technique of arbitrary event attributes versa arrival time enabling an operator to analyze the event history. A distinct disadvantage of this method is that only one of the event attributes may be plotted versus the arrival time of the events. Thus, the operators have to switch continuously between the various event attributes to make sure that they do not miss a significant event pattern. The disadvantages of S. Ma et al., are overcome with the invention claimed in claims 1-15. Often, the passages cited in the office action apparently fail to show what is alleged in the office action. Thus claims 1-15 are allowable.

In particular, claim 1 reads,

> 1. (original) A method of monitoring events in a computer network, the method comprising:
>
> said computer network triggering said events, each event being provided with attribute values allocated to a given set of attributes,
>
> providing an event display with a cross plot having x and y coordinate axes, the x-axis presenting a time period and the y-axis presenting an attribute value range,
>
> determining a primary attribute of the events selected from the given set of attributes to be presented with its attribute values on the y-axis of the cross plot,
>
> allocating a first display label to the events indicating the attribute values of the primary attribute, providing a pattern algorithm to detect whether an arrived event is part of the given pattern on the basis of a comparison of the attributes allocated to the given pattern and of the attributes assigned to the arrived event, providing a mapping algorithm to map any attribute value of an attribute selected from the given set of attributes onto the y-axis of the cross plot,
>
> allocating a second display label to the events indicating the attribute values of the attributes being uncovered as part of the given pattern, plotting all the events arrived within the time period and including an attribute value allocated to the primary attribute into the cross plot with the first display label indicating the primary attribute, the position

of the first display label of each event in the cross plot being determined on the basis of the attribute value of the primary attribute of the event and its arrival time, and

plotting the all events arrived within the time period and being detected by means of the pattern algorithm as part of the given pattern into the cross plot with the second display label indicating the given pattern, the position of the second display label of each event in the cross plot being determined by the mapping algorithm on the basis of the attribute value of the attribute of the event being uncovered as part of the given pattern and its arrival time.

This is not in Ma. The office action reads:

> *Claim 1: Ma teaches a method of monitoring events in a computer network, the method comprising:*
>
> *Said computer network triggering said events, each event being provided with attribute values allocated to a given set of attributes (See Page 1, second paragraph, for attribute values, see the last paragraph of Page 6 and the first and second paragraphs of Page 8 and the real data set collected from a production computer network containing thousands of managed nodes including routers, hubs and servers are described in the last paragraph of page 3 and identifying unknown event patterns that can be used for real-time monitoring is described in the second paragraph of page 3);*
>
> *Providing an event display with a cross plot having x and y coordinate axes, the x-axis presenting a time period and the y-axis present an attribute value range (e.g., Figs. 2,4,6,7 and the third paragraph of Page 8 describes a scatter plot or cross plot having an y-axis representing around 160 hosts of a communication network and the x axis has been described in the figures as well as the first paragraph of page 6; for attribute value rang; see these figures as well as the description in the second paragraph of Page 8);*
>
> *Determining a primary attribute of the events selected from the given set of attributes to be presented with its attribute values on the y-axis of the cross plot (e.g., attributes including the categorical attributes or temporal attributes such as the host names and the primary attribute values are displayed in Figs. 2, 4, 6 and 7 and multiple attributes are described in the last paragraph of Page 11),*

In response, applicants respectfully state that there is apparently no indication that Ma. Performs a step of determining a 'primary attribute', as in claim 1. In claim 1, in order to differentiate the events associated with the primary attribute from the events being part of the interesting event pattern, a first display label is assigned to all events including a primary attribute value and a second display label is assigned to all events indicating the attribute values of the attributes being uncovered as part of the relevant event pattern. By using the inventive method of monitoring events, the event display presents a plot of information of the main event attribute versus the arrival time of the event by using a first display label for the plotted events wherein the interesting event pattern derived from other event attributes is simultaneously presented by using the second display label for these events. If the operator of the intrusion detection system wants to investigate the events being detected as part of a given pattern in more detail, he can easily switch to the corresponding event attribute by selecting a mark of the second display label in the cross plot.

The office action reads:

> *Allocating a first display label (e.g., Pattern 1, Pattern 2, Pattern 3 and Pattern 4 are marked in the scatter plot or the cross plot of Fig. 7) to the events (e.g. alarms in Page 10) indicating the attribute values of the primary attribute (key attribute values are described in the second paragraph of page 3 and other attribute values are also described there), providing a pattern algorithm (the pattern algorithm is described in Fig. 7 as well as the mining algorithm as described in the last paragraph of page 12 or the EventMiner) to detect whether an arrived event (arrived event are the selected event objects or the selected data objects in a specific time range related to the events progressively loaded from a database or the mining alarm logs in a real time system; see first paragraph of page 13 and the last paragraph of page 10 and a new query that retrieves the relevant data objects for more analysis in which a new query is restricted to a range constraint for a numerical attribute; see the last paragraph of page 10) is part of the given pattern (is part of the part of the given pattern such as the Pattern 1 or the Pattern 2) on the basis of a comparison of the attributes allocated to the given pattern and of the attributes assigned to the arrived event (coloring events by the coloring and filtering algorithm or the data mining algorithm and comparing the difference or similarity in terms of patterns indicated by colors; see page 13), providing a mapping algorithm to map any attribute value of an attribute selected from the given set of attributes onto the y-axis of the cross plot (see the last paragraph of Page 11),*

In response, applicants respectfully state that there is apparently no indication that Ma. Performs a step related to a 'primary attribute', as in claim 1. *Although Ma has a display, Ma apparently do not*

allocate a "display label to the events indicating the attribute values of the primary attribute," nor do Ma provide, "a pattern algorithm to detect whether an arrived event is part of the given pattern on the basis of a comparison of the attributes allocated to the given pattern and of the attributes assigned to the arrived event, ...etc.

> *Allocating a second display label (e.g.. Pattern 2) to the events indicating the attribute values of the attributes being uncovered as part of the given pattern, plotting all the events arrived within the time period and including an attribute value allocated to the primary attribute into the cross plot with the first display label indicating the primary attribute the position of the first display label of each event in the cross plot being determined on the basis of the attribute value of the primary attribute of the event and its arrival time (see Figs. 2,4,6, and 7 and the related paragraphs mentioned above in "allocating a first display label"), and Plotting the all events arrived within the time period (Figs. 2, 4, 6, and 7 plot the all events within a specific time range) and being detected by means of the pattern algorithm (by the event miner algorithm) as part of the given pattern into the cross plot with the second display label (e.g., Pattern 2 or the Green Spike in Fig. 10), the position of the second display label of each event in the cross plot being determined by the mapping algorithm on the basis of the attribute value of the attribute of the event (see Fig. 10) on the basis of the attribute value of the attribute of the event being uncovered (uncovered for example in the alarm log and uncovered by the mining algorithm) as part of the given pattern and its arrival time (all the selected events are in a specific time range as plotted in Figs. 2,4,6.7 and 10).*

In response, applicants respectfully state that there is apparently no indication that Ma. Performs a step related to a 'primary attribute', as in claim 1. Although Ma has a display, Ma apparently do not have a second display. The 'Pattern 2' of Ma, is not concerned with the second display of claim 1's step of "allocating a second display label to the events indicating the attribute values of the attributes being uncovered as part of the given pattern, plotting all the events arrived within the time period and including an attribute value allocated to the primary attribute into the cross plot with the first display label indicating the primary attribute, the position of the first display label of each event in the cross plot being determined on the basis of the attribute value of the primary attribute of the event and its arrival time."

Nor is the plot of Ma, concerned with the step of claim 1 for, "plotting the all events arrived within the time period and being detected by means of the pattern algorithm as part of the given pattern into the cross plot with the second display label indicating the given pattern, the position of the second display label of each event in the cross plot being determined by the mapping algorithm on the basis of the attribute value of the attribute of the event being uncovered as part of the given pattern and its arrival time." In the method of Ma, **only one of the event attributes may be plotted versus the arrival time of the events.** Thus, the operators have to switch continuously between the various event attributes to make sure that they do not miss a significant event pattern. The disadvantages of S. Ma et al., are overcome with the invention claimed in claims 1. Thus, claim 1 and all claims that depend on claim 1 are allowable.

> *Re Claims 2-3:*
> *Ma farther discloses selecting the new events within the specified time period and plotting the new events within the shifted time period into the cross plot (See Figs. 6,7,9 and 10 in which events in the two time periods are drawn and the spikes are identified and the newly selected events are redrawn as determined by the data mining algorithm for the time period during which the new events are retrieved).*

In response, applicants respectfully state that claims 2 and 3 read,

> 2. The method according to claim 1, further comprising:
>
> recording the attribute values and the arrival time of a new event, determining on the basis of the recorded attribute values of event whether or not the newly arrived event includes an attribute value of the primary attribute, and if the newly arrived event includes the attribute value for the primary attribute shifting the x-axis of the cross plot so that the time period being presented on the x-axis covers the arrival time of the event, and
>
> plotting the event arrived within the shifted time period into the cross plot with the first display label indicating the primary attribute.
>
> 3. The method according to claim 2 comprising the further steps of:
>
> determining on the basis of the recorded attribute values of event whether or not the newly arrived event is part of the given pattern on the basis of a comparison of the

attributes allocated to the given pattern and of the attributes assigned to the arrived event,

if the newly arrived event includes an attribute value of the given pattern adding the event to the previous events being detected as part of the given pattern, and

redrawing all the events being associated with given pattern in the cross plot.

As noted Ma's method is that only one of the event attributes may be plotted versus the arrival time of the events. Thus, the operators have to switch continuously between the various event attributes to make sure that they do not miss a significant event pattern. Ma is not concerned with the 'primary attribute' nor for a plurality of event attributes, as in claims 2 and 3 which are allowable over Ma et al.

Re Claims 4-5:
Ma farther discloses the third display label and the fourth display label indicating the new patterns (See the three colored spikes in Fig. 6 and the four patterns in Fig. 7).

In response, applicants respectfully state that the indicating of new patterns in Ma, is not the steps of claim 4. Ma do not test as in claim 4, "if the newly arrived event does not include an attribute value of the given pattern." Nor do Ma determine, "**on the basis of the recorded attribute values of all previous arrived events by means of the pattern algorithm whether or not the newly arrived event is part of a new pattern on the basis of a comparison of the attributes allocated to the new pattern and of the attributes assigned to the arrived events.**" Nor do Ma test, "if the newly arrived event forms together with previous recorded events the new pattern," Nor do Ma allocate, "a third display label to the events indicating the attribute values of the attributes being uncovered as part of the new pattern." Certainly, Ma does apparently not perform the step of, "**plotting the all events being detected by means of the pattern algorithm as part of the new pattern into the cross plot with the third display label indicating the new pattern**, the position of the third display label of each event in the cross plot being determined by the mapping algorithm on the basis of the attribute value of the attribute of the event being uncovered as part of the new pattern and its arrival time. Thus claim 4 is allowable over Ma.

Similarly, Ma are not concerned with a 'primary attribute nor with the step of claim 5, of **removing all the events including an attribute value allocated to the primary attribute from the cross plot,** if a primary attribute to be presented with its attribute values on the y-axis of the cross plot is changed, allocating a fourth display label to the events indicating the attribute values of the new primary attribute," nor with the step of, "plotting all the events arrived within the time period and including an attribute value allocated to the new primary attribute into the cross plot with the fourth display label indicating the new primary attribute, the position of the fourth display label of each event in the cross plot being determined on the basis of the attribute value of the primary attribute of the event and its arrival time," nor with the step of, "if a primary attribute to be presented with its attribute values on the y-axis of the cross plot is changed, allocating a fourth display label to the events indicating the attribute values of the new primary attribute, and plotting all the events arrived within the time period and including an attribute value allocated to the new primary attribute into the cross plot with the fourth display label indicating the new primary attribute, the position of the fourth display label of each event in the cross plot being determined on the basis of the attribute value of the primary attribute of the event and its arrival time. Thus claim 5 is allowable over Ma.

> *Re Claim 6:*
> *Ma further discloses the operator selects the events to be plotted and displaying textual and coloring information associated with the selected events on the event display (Page 4 and Figs. 6,7,9-10).*

In response, applicants respectfully state that claim 6 reads,

> 6. The method according to claim 1 comprising the further steps of plotting all attribute values recorded for an event with the respective display label into the cross plot if the event is selected by an operator, and displaying textual information associated with the selected event on the event display.

Ma is not concerned with the test and step of claim 6 of, "plotting **all attribute values recorded for an event with the respective display label into the cross plot if the event is selected by an**

operator, and displaying textual information associated with the selected event on the event display. Thus claim 6 is allowable over Ma.

Re Claim 7:
Ma further discloses a pattern algorithm such as the data mining algorithm suitable to perform multi-attribute pattern recognition (Figs. 6,7, 9.10).

In response, applicants respectfully state that claim 7 reads,

> 7. The method according to claim 1, wherein the pattern algorithm is suitable to perform multi-attribute pattern recognition.

There is apparently no indication that Ma is concerned with *multi-attribute pattern recognition* or even any *pattern recognition*. Being allegedly suitable is indeed not an anticipation of the invention in claim 7. Thus claim 7 is allowable over Ma.

Re Claim 8:
Ma further discloses using color such as Red and Green to color the pattern Spikes and Pattern 1, Pattern 2, Pattern 3, Pattern 4 for specific mark layouts (Figs. 6,7.9-10).

In response, applicants respectfully state that claim 8 reads,

> 8. (original) The method according to claim 1, wherein each display label includes a specific color and/or a specific mark layout.

Ma's use of colors is apparently not similar or anticipate of the use of color in claim 8. Thus claim 8 is allowable over Ma.

Re Claim 9:
Ma farther discloses all events being uncovered as part of the pattern being clustered by the display label such as Red Spikes, Green Spikes (Figs. 6,7 and 9-10).

In response, applicants respectfully state that claim 9 reads,

> 9. (original) The method according to claim 1, wherein all events being uncovered as part of the pattern are clustered by the corresponding display label.

There is apparently no indication that Ma is at all concerned with clusters or clustering as in claim 9. Thus claim 9 is allowable over Ma.

Re Claim 10:

Ma further discloses a data mining algorithm and GUI(page 14).

In response, applicants respectfully state that the response to claim 1 is appropriate to claim 10 which depends thereupon. The program code is the that of claim 1, which is not anticipated by Ma. Thus claim 10 is allowable over Ma.

Re Claim 11:
Ma further discloses the program code being stored on data carrier (see page 5).

In response, applicants respectfully state that there is apparently no indication that Ma discloses or is concerned with a data carrier as in claim 11. Thus claim 11 is allowable over Ma.

Re Claim 12:
Ma further discloses an event visualization device for monitoring events in a computer network (Page 3).

In response, applicants respectfully state that the response to claim 1 is appropriate to claim 12, which depends thereupon. The device is for performing the steps of claim 1, which is not anticipated by Ma. Thus claim 12 is allowable over Ma.

Re Claims 13-15:
Ma farther discloses an implementation of the Event Miner algorithm on the computer (Page 4-5).

In response, applicants respectfully state that the response to claim 1 is appropriate to claims 13-15, which depends thereupon. The article of manufacture of claim 13 is for performing the steps of claim 1, which is not anticipated by Ma. The program storage device of claim 14 is for performing the steps of claim 1, which is not anticipated by Ma. The product of claim 15 is for performing the functions of claim 12, which is not anticipated by Ma. Thus claims 13-15 are allowable over Ma.

Thus these claims and all claims that depend upon these claims are allowable over the cited art. Thus, claims 1-15 are allowable. Claims 16-20 are added. A listing of the claims is provided as required in the new USPTO amendment practice per 37 CFR 1.121.

It is anticipated that this amendment brings the application to allowance of claims 1-20. Favorable action is respectfully solicited. In the unlikely event that any claim remains rejected, please contact the undersigned by phone in order to discuss the application.

Please charge any fee necessary to enter this paper to deposit account 50-0510.

Respectfully submitted,

By: Louis Herzberg

Dr. Louis P. Herzberg
Reg. No. 41,500
Voice Tel. (845) 352-3194
Fax. (914) 945-3281

3 Cloverdale Lane
Monsey, NY 10952

Customer Number: 54856